REMARKS

This communication is in response to the Examiner's Answer mailed July 3, 2008, in which the Examiner has set forth a new ground of rejection. This communication is also in response to an interview with Examiner J. Kucab, by Applicant's attorney Jonathan O. Scott, Reg. No. 39,364 and Jubin Dana, Reg. No. 41,400 on August 14, 2008. This is a request under 37 CFR 41.39(b)(1) to reopen prosecution.

During the interview, the new ground of rejection was discussed. In addition, the eighth step of claim 1 was discussed. In addition, the Carrott reference was generally discussed.

To address the rejection under 35 USC 101, which is the new ground of rejection advanced in the Examiner's Answer, Applicant has amended the independent method claims to include a "trusted party computer."

Furthermore, the claims have been amended to clarify, with regard to the profile data, "said presenter having transmitted said profile data to said trusted party," as requested by the Examiner during the interview. In addition, the claims have been amended to emphasize that the notifying the acceptor by the trusted party, regarding the presenter, is "during said on-line transaction and in real time." As set forth in the Examiner's Answer, the claims remain rejected under 35 USC 103 as being unpatentable over Carrott et al. (Carrott) in view of Tsuei et al. (Tsuei).

With regard to claim 1, the eighth step recites "validating, by said trusted party, said submitted profile data using results of said comparing and results of said authenticating." Thus, the validating step uses the result of comparing (the submitted profile data against the profile data stored by the trusted party) and the result of authenticating (the presenter) in order that validation be successful. Even if perhaps Carrott can be considered to disclose comparing the user profile with a profile from the merchant, Carrott certainly does not also check at the same time, again, the user's authentication data in order to confirm the validation. Claim 1 requires both checks for validating the submitted profile data; the advantage is that the presenter must not only authenticate his or her identity during enrollment, but also during submission of profile data during the online transaction in real time. Carrot does not authenticate the presenter a second time during comparison of the profile data.

Furthermore, claim 23, dependent on claim 1, further recites "providing, by said trusted party, of updated profile data when said submitted profile data is determined to be out of date." The Examiner refers to Carrott's col. 2, lines 25-33, as allegedly disclosing such a feature. Carrott's col. 2, lines 25-33 discloses:

> If authorization is not approved, on the basis of incorrect address information, the options to the financial institution include: 1) approving the transaction with the corrected address; 2) approving the transaction subject to the customer updating his/her address information prior to the issuance of the authorization code; and, 3) declining authorization.

While this section discloses the "customer updating his/her address information," the user updating his/her address does not correspond to the feature in claim 23 of the trusted party providing updated profile data when the submitted profile data is determined to be out of date.

Regarding claim 9, this claim is dependent on claim 1 and further recites:

> providing, by said trusted party, to said presenter a program identity number which is correlated with said profile data and said authentication data; and
> storing said program identity number by said trusted party.

This allows the trusted party to match up the submitted profile data with the stored profile data. For example, in Applicant's specification at page 7, lines 27-30, it is stated:

> Presenter file database 722 is a database managed by the trusted party 710 that stores information relating to the presenters that are successfully enrolled in the data authentication services program. Such information includes program identity numbers, profile data, and passwords.

At page 8, line 26 to page 9, line 5 of Applicant's specification, it is further stated:

> A presenter registers with a trusted party to be eligible to use the data authentication services program. Upon successful registration, a trusted party provides a presenter with a program identity number and an authenticating password, token, or other authenticating mechanism. A program identity number is a number that identifies presenters who are properly enrolled to use the authentication services program. A program identity number can be any type of number such as a random number or a number issued out of a series of numbers. In one embodiment of the invention, the program identity number can also be a payment card number. This is convenient in the case where presenter 708 is a payment card cardholder and trusted party 710 is the issuing bank of the payment card. An authenticating password, token, or other authenticating mechanism allows trusted party 710 to authenticate the identity of a presenter 708 since only trusted party 710 and presenter 708 know the password, token, or other authenticating mechanism.

The Examiner contends, with regard to Tsuei, that "Tsuei teaches a system wherein the program identity is an account number of financial account wherein the trusted third party maintains said account." However, nothing in Tseui discloses or suggests that the "account number" is

"correlated with said profile data and said authentication data" as recited in claim 9. A similar feature is recited in claims 29 and 44.

Regarding claim 37, this claim recites, in part (emphasis added):

providing said profile data of said presenter, by said trusted party, to said acceptor; and

notifying said acceptor by said trusted party of the authenticity of said presenter during said on-line transaction and in real time, whereby said trusted party authenticates said presenter for the benefit of said acceptor and provides said profile data.

Claim 52 has a similar recitation. Put simply, regarding these claims 37 and 52, the acceptor does not have the profile, but is asking the trusted party for the profile. Carrott, on the other hand, discloses that the central party verifies the profile data from the merchant but, significantly, does not supply the profile data for a customer to a merchant. Because Carrott does not disclose this step of providing profile data to the acceptor, it is requested that rejections of claims 37 and 52 be withdrawn.

CONCLUSION

Applicant respectfully requests consideration of the amendments and arguments set forth herein.

In the first place, it is respectfully submitted that the new ground of rejection set forth in the Examiner's Answer has been adequately addressed.

Furthermore, Applicant requests consideration of the arguments set forth herein with respect to the claimed subject matter, as compared to the cited Carrott and Tsuei references. It is respectfully submitted that, for at least the reasons set forth herein, as well as for the reasons set forth in the Appeal Brief and prior communications submitted by Applicant during prosecution, that the claimed subject matter is patentable over Carrott and Tsuei.

Consideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested.

Respectfully submitted,
BEYER LAW GROUP LLP

/ASH/
Alan S. Hodes
Reg. No. 38,185

P.O. Box 1687
Cupertino, CA 95015-1687
(408) 255-8001